UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/762,544	01/23/2004	Yukie Gotoh	2004-0089A	4981

513 7590 07/24/2008

WENDEROTH, LIND & PONACK, L.L.P.
2033 K STREET N. W.
SUITE 800
WASHINGTON, DC 20006-1021

EXAMINER	
HOMAYOUNMEHR, FARID	

ART UNIT	PAPER NUMBER
2139	

MAIL DATE	DELIVERY MODE
07/24/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/762,544	GOTOH ET AL.	
	Examiner	Art Unit	
	Farid Homayounmehr	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 January 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *23 January 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *multiple*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-34 have been examined.

Information Disclosure Statement PTO-1449

2. Information disclosure statements submitted by applicant dated 1/23/2004, and 7/12/2004 were considered. Please see attachment PTO-1449.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Friedman (U.S. Patent No. 6,240,513, dated 5/29/2001) in view of Chmielewski (U.S. Patent No. 5,946,465, dated 8/31/1999), hereinafter called Chei.

4.1. As per claim 1, Friedman is directed to a common key exchanging method for exchanging a common key between two communication devices for transmission and reception of encrypted/authenticated data (col. 5 lines 8-15, or col. 10 lines 12-20), comprising: an information transmitting step, performed by at least one of the communication devices, of transmitting information required for another one of the

communication devices to acquire the common key to the other one of the communication devices (col. 9 lines 20-30 and also Fig. 8 and associated text, namely col. 12 lines 32 to col. 13 line 15);

a setting step, performed by said at least one of the communication devices, of setting a waiting limit for a response from the other one of the communication devices based on a time required for a predetermined operation to be performed by the other one of the communication devices by a next response timing (col. 13 lines 15-37 shows the setting of a wait period after the information (the static or dynamic public keys) are sent. If the wait time expires, the packet is dropped. If a reply is received, it will be used to generate the common key using Diffie-Hellman protocol. Therefore, Friedman teaches setting a wait time limit for a response from the other device. Note also that the Diffie-Hellman protocol generates the common key based on the public key received from the other device. Therefore, the wait time is logically based on the time required for the other device to send its public key. However, Friedman does not explicitly state that the wait time is based on the time required by the other device to send its public key. Chei is directed to a system that **calculates** a wait time based on responses from the other device (see col. 2 lines 5-21). Specifically, Chei's system calculates this wait time so that the resources associated with an inactive connection can be released and used for active connections (see col. 1 line 60 to col. 2 line 5). Chei col. 3 line 6 to col. 5 line 20 teach that the wait time is based on the time it takes for the response from the other to arrive. This teaches the concept that when it is possible to calculate the time it takes to

receive a response from the other device, it is desirable to calculate a wait time accordingly, and start reusing the resources after such wait time is expired. Friedman and Chei are analogous art, as they are both directed to establishing reliable network connections between communication devices. At the time of invention, it would have been obvious to the one skilled in art to combine the teachings of Chei, which is calculating an expected response time from the other device, in the system of Friedman to set the wait time based on the expected response time from the other device. The motivation, as stated by Chei, would be to reuse system resources dedicated to an idle connection. Note once again, that Friedman's invention is about establishing a common key between the communicating device, and the wait time is logically set for the time it is needed to receive the public key of the other device);
an acquiring step, performed by the other one of the communication devices, of acquiring the common key from the information by performing the predetermined operation; and a response transmitting step, performed by the other one of the communication devices, of transmitting a predetermined response to the one of the communication devices in the next response timing (col. 14 lines 25-47. Also note that the common key is calculated by each device, after receiving a response from the other device (containing the public key of that device) as explained in col. 13 lines 21-28).

4.2. As per claim 2, Friedman is directed to the common key exchanging method according to claim 1, wherein each of the communication devices calculates its own public value for transmission to the other, and calculates the common key based on the

public value received from the other, thereby achieving an exchange of the common key (the Diffie-Hellman protocol as explained in claim 1), and in the setting step, the waiting limit is set based on at least either one of a time required for calculation of the public value performed by the other one of the communication devices and a time required for calculation of the common key performed by the other one of the communication devices (see response to claim 1, and note that the source device needs the response from the other device to calculate the common key).

4.3. As per claim 3, Friedman is directed to the common key exchanging method according to claim 1, wherein the one of the communication devices encrypts a common key generated by a unit included in the one of the communication devices or information for generating the common key and transmits the encrypted common key or the encrypted information, and the other of the communication devices decrypts the encrypted common key or the encrypted information to generate a common key and transmits a response of acknowledging the common key to the one of the communication devices, thereby achieving an exchange of the common key (Friedman col. 12 lines 32-42 shows encrypting the dynamic public key (information for generating the common key) by the static key before transmission to the other device. Col. 14 lines 25-33 shows that the other device extracts the information to generate the common key. To perform the Diffie-Hellman protocol, the dynamic public key must be available in clear form, and therefore the other device must decrypt the encrypted dynamic public key to access the dynamic public key),

and in the setting step, the waiting limit is set based on a time required for decryption of the encrypted common key or a time required for decryption of the encrypted information and generation of the common key performed by the other one of the communication devices (as indicated in the response to claims 1 and 2, the wait time is calculated to match the time it is required to complete and receive the response from the other device. The source encrypts the information before sending it. Therefore, it would be logical to consider the decryption time included in the total response time expected from the other device. The same applies to any additional process included in the key exchange process).

4.4. As per claim 4, Friedman is directed to the common key exchanging method according to claim 1, wherein after receiving a request message from the one of the communication devices, the other one of the communication devices encrypts the common key or information for generating a common key by using a public key received from the one of the communication devices and transmits the encrypted common key or the encrypted information to the one of the communication devices, thereby achieving an exchange of the common key, and in the setting step, the waiting limit is set based on a time required for encryption of the common key or the information for generating the common key (see response to claims 1-3 and note that Diffie-Hellman requires both parties to exchange information necessary to generate the common key. Therefore, the other device performs the same activities as the source side).

4.5. As per claim 5, Friedman is directed to the common key exchanging method according to claim 1, wherein the predetermined operation is either one of an operation for an authentication process associated with acquisition of the common key and an operation for acquisition of the common key and the authentication process accompanied thereby (encrypting the dynamic key using the static key is considered authenticating the dynamic key).

4.6. As per claim 6, Friedman is directed to the common key exchanging method according to claim 5, wherein the one of the communication devices transmits data with a digital signature for authentication to the other one of the communication devices, and the other one of the communication devices performs an identity authentication process based on the data with the digital signature received from the one of the communication devices, thereby achieving the authentication process, and in the setting step, the waiting limit is set based on a time required for the identity authentication process performed by the other one of the communication devices (once a common secret (such as the static public key) is established between the parties, inclusion of any well-known cryptographic process, such as digital signatures, to enhance the security level of the key exchange protocol would be obvious to the one skilled in art).

4.7. As per claim 7, Friedman is directed to the common key exchanging method according to claim 5, wherein the one of the communication devices transmits data using public key encryption for authentication to the other one of the communication devices, and the other one of the communication devices performs an identity authentication process based on the data using public key encryption received from the one of the communication devices, thereby achieving the authentication process, and in the setting step, the waiting limit is set based on a time required for the identity authentication process performed by the other one of the communication devices (see response to claim 6).

4.8. As per claim 8, Friedman is directed to the common key exchanging method according to claim 1, further comprising:
an estimating step, performed by the other one of the communication devices, of estimating a required operation time to be taken for the predetermined operation; a time transmitting step, performed by the other one of the communication devices, of transmitting the estimated required operation time to the one of the communication devices; and a receiving step, performed by the one of the communication devices, of receiving the required operation time from the other one of the communication devices (Chei Fig. 3 and associated text teach an estimation of the expected response time form the other device).

4.9. As per claim 9, Friedman is directed to the common key exchanging method according to claim 8, further comprising a
step, performed by the one of the communication devices, of making an inquiry of the other one of the communication devices about the required operation time, wherein in response to the inquiry from the one of the communication devices, the other one of the communication devices performs the estimating step and the time transmitting step (Freidman in view of Chei teaches setting a wait time based on the time expected to receive a response from the other device, such that the idle resources can be used more efficiently. An essential part of this process is obtaining an expected time to receive a response from the other device. Inquiring the other device about the expected response time would have been an obvious alternative for obtaining an expected response time. The obvious choices of determining the response time of the other device include performing an estimation response time by the other device, having the response time stored in the other device, and dynamically adjusting the response time to include processing delays, network transmission delays, etc.).

4.10. As per claim 10, Friedman is directed to the common key exchanging method according to claim 8, wherein the other
one of the communication devices stores in advance the required operation time (see response to claim 7).

4.11. As per claim 11, Friedman is directed to the common key exchanging method according to claim 1, further comprising:
a step, performed by the other one of the communication devices, of transmitting at least once to the one of the communication devices a report that a response will be delayed by the next response timing; and a step, performed by the one of the communication devices, of receiving the report from the other one of the communication devices, wherein in the setting step, a waiting limit for the response is set based on the report (see response to claim 9)

4.12. As per claim 12, Friedman is directed to the common key exchanging method according to claim 1, further comprising:
a step, performed by the one of the communication devices, of measuring a time starting at a time of transmitting a message and ending at a time of receiving a response after the predetermined operation from the other one of the communication devices, so as to obtain a time to be taken for the predetermined operation (Chei Fig 3 and associated text teach measuring the response time).

4.13. As per claim 13, Friedman is directed to the common key exchanging method according to claim 2, wherein the public value and the common key are calculated by the other one of the communication devices by the next response timing, and in the setting step, awaiting limit for a response with regard to transmission of the public value

or completion of calculation of the common key is calculated based on a total time to be taken for calculation of the public value and the common key performed by the other one of the communication devices (see response to claim 9).

4.14. As per claim 14, Friedman is directed to the common key exchanging method according to claim 2, wherein the public value is calculated by the other one of the communication devices by the next response timing, and in the setting step, a waiting limit for a response with regard to transmission of the public value or completion of calculation of the common key is calculated based on a time to be taken for calculation of the public value performed by the other one of the communication devices (see response to claim 9).

4.15. As per claim 15, Friedman is directed to the common key exchanging method according to claim 2, wherein the common key is calculated by the other one of the communication devices by the next response timing, and in the setting step, a waiting limit for a response with regard to transmission of the public value or completion of calculation of the common key is calculated based on a time to be taken for calculation of the common key performed by the other one of the communication devices (see response to claim 9).

4.16. As per claim 16, Friedman is directed to the common key exchanging method according to claim 2, further comprising:
a step, performed by each one of the communication devices, of transmitting a completion report to the other after calculation of the common key has been completed; and a step, performed by each one of the communication devices, of refraining from determining whether a key exchanging process has failed until a completion report is received from another one of the communication devices (see response to claim 9, and note that as mentioned in response to claim 1, the purpose of Freidman in view of Chei is calculating a close estimate of response time such that the connection is not terminated too soon or too late. Terminating a connection too soon would also be a waste of resources, as setting up the connection requires resources).

4.17. As per claim 17, Friedman is directed to the common key exchanging method according to claim 2, wherein the
information transmitting step, the setting step, the acquiring step, and the response transmitting step are preformed in a message sequence in the IKE (IKE is the standard protocol to exchange keys, which uses Diffie-Hellman protocol. It would have been obvious to the one skilled in art to use the tools provided in a standard protocol to complete the key exchange).

4.18. The requirements of claims 18-34 are substantially the same as claims 1-17 above.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Farid Homayounmehr whose telephone number is 571 272 3739. The examiner can normally be reached on 9 hrs Mon-Fri, off Monday biweekly.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kristine Kincaid can be reached on (571) 272-4063. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Farid Homayounmehr

Examiner

Art Unit: 2139

/Kristine Kincaid/

Supervisory Patent Examiner, Art Unit 2139